Audit Follow-up: Mobile Computing Security

September 2015 FY15 - #07

Submitted to:
Michele L. Norin, Vice President for Information Technology and Chief Information Officer
Derek A. Masseth, Senior Director, Cloud Services, University Information Technology Services

Copies to:
Audit Committee, Arizona Board of Regents
Andrew C. Comrie, Senior Vice President for Academic Affairs and Provost
Gregg Goldman, Senior Vice President for Business Affairs and Chief Financial Officer
Laura Todd Johnson, Vice President, Legal Affairs and General Counsel
Jon Dudas, Senior Associate to the President and Secretary of the University
Duc D. Ma, Interim Associate Vice President, Financial Services Office

Issued by: Sara J. Click, CPA, Chief Auditor
Internal Audit Department

Audit Follow-up: Mobile Computing Security

Summary

Follow-up on prior audits was included in our Fiscal Year ("FY") 2015 Audit Plan. The professional standards for internal auditing require auditors to follow-up on any recommendations included in prior audit reports.

Background: Internal Audit completed audit report, FY13 - #13, that evaluated the policies, practices and controls in place for mobile computing security. The audit was included in our approved FY 2013 Audit Plan. The audit report included management responses ("Action Plan") to our recommendations and target implementations dates from the Office of the Chief Information Officer ("CIO"). The Office of the CIO includes University Information Technology Services ("UITS") and the Information Security Office ("ISO").

The audit report contained a finding related to the assessment of information security policies, specifically data classification and protection requirements. The second finding included high-risk areas of Information Technology ("IT") and the governance processes in place to ensure effective and informed decisions. These services include cloud storage systems, virtual private networks ("VPN"), application vulnerability testing, mobile device management, and the use of personal devices to conduct University business.

Audit Objective: To evaluate whether the open Action Plan items from the November 2013 Action Plan were implemented and functioning as intended.

Methodology: We accomplished our objective by providing the CIO with a listing of the Action Plan items on a *Departmental Action Plan Status Form*. The high risk and complexity of the findings required several meetings and review of submitted materials to evaluate the response and associated risk. Several iterations of the Action Plan were submitted, reviewed, and discussed prior to acceptance of the final document.

Conclusion: We found that the Office of the CIO made considerable progress on the Action Plan. Some actions have been completed, and others are considered partially complete as additional time is required for discussion with University executive management.

The recommendation for the first finding was for the ISO to validate that information security policies sufficiently addressed mobile computing. The Data Classification Standard (IS-101) is critical component of the Information Security policy. Data classification supports the University community's awareness of the risks associated with data management and the University's expectations for protecting data.

The data classification standard was modified to include four classifications of data: *public, internal, confidential and regulated*. The requirements for protecting and storing the data are included in the document. The updated data classification standard became effective on March 20, 2015.

The second finding relates to IT governance for high-risk IT areas in the University's heavily decentralized IT model. There are several actions included in this finding. While many actions remain open, much work has been done toward reducing risk. Highlights of items completed to date are listed below:

- The CIO has made considerable progress in establishing and formalizing IT governance for the University. Actions include the creation of an IT governance matrix and establishing various committees such as the Executive Coordinating Group and the Business Systems Coordinating Council.

- The updated Data Classification Standard includes expanded classifications and guidance for using cloud services.

- Configuration changes to the enterprise VPN service were made to ensure that security settings were appropriate. Currently, the idle time-out is after 24 hours of inactivity, which allows the connection to remain active with all enterprise systems and services accessible. A 24-hour session limit and a four-hour idle limit are under consideration to further reduce risk.

Due to the high risk of the open action items, additional follow-up will be required.

/s/
Rosemary R Casteel, CISA
Auditor-In-Charge
(520) 626-4235
casteelr@email.arizona.edu

/s/
Sara J. Click, CPA
Chief Auditor
(520) 626-4155
clicks@email.arizona.edu

Attachment: *Departmental Action Plan Status Form*

Departmental Action Plan Status Form
Internal Audit of Mobile Computing Security (Issued November 2013)

Please complete the right side of this form indicating the status of each of the action plan items listed on the left. As a convenience, action plan items are listed and referenced in the same order as they appear in the audit report. For any items that have not been implemented, please indicate the targeted date or the alternate solution implemented.

ACTION PLAN **(From the Audit Report)**	**CURRENT STATUS** **(Include Each Action Plan Item)**
FINDING #1: The effects of mobile computing, while conducting University business have not been formally assessed University-wide to determine the impact on information security policies. **Target Implementation Date:** December 2014 **Original Response (November 2013):** We agree that appropriate staffing levels should be maintained so that regular reviews of and updates to policies, standards, guidelines, and procedures can be completed in a timely manner. We have already begun interviews for a new *Manager, Information Assurance* position which will be responsible for updating and enhancing the University-wide information security policy framework. We anticipate the review of the Data Classification Standard by December 2014. Additionally, the Information Security Strategic Plan has identified staffing needs over the coming years. This plan will be updated periodically to reflect recommended staffing levels to best meet the information security risk management obligations of the University.	**Management Update: Complete** A *Manager for Information Assurance* was hired in March 2014. Review of the existing Data Classification Standard was completed by August 2014, and a new 4-tier data classification model was established in March 2015. In addition, a file-sharing guide is available outlining which sharing services can be used for each classification of data. All can be found online at http://security.arizona.edu/data-classification-and-handling-standard. The information security teams from the University of Arizona, Arizona State University, and Northern Arizona University have agreed to collaborate and adopt a modified version of the "**Framework for Improving Critical Infrastructure Cybersecurity**" published by the National Institute of Standards and Technology (NIST) in February 2014. The 4-tier data classification model and the NIST cybersecurity framework will serve as the basis for helping campus units make risk-based information protection decisions. Expansion of the 4-tier

	classification model and implementation of the NIST cybersecurity framework will be an ongoing effort facilitated through regular meetings of the IT Security Council, a governance group made up of designated IT leaders from the dozens of academic and administrative units across the University.
FINDING #2: The current level of IT governance is not sufficient to manage the decentralized IT model and to ensure that confidential data is protected. **Target Implementation Date:** December 2014 **Original Response (November 2013):** We agree to define an IT governance structure and decision-making process by December 2014, along with a plan for implementation. The CIO will initiate a series of discussions with University administration and key campus stakeholders to determine need, level and type of participation and possible guidelines for decision-making. Currently, IT strategies, issues and decisions are discussed among the various key stakeholders and committees across campus. Any new formalized IT governance structure will take these steps into consideration and if it is determined that a more formalized structure is desired, then implementation will occur accordingly within a reasonable timeframe. Each of the areas listed above will be addressed either through existing decision making processes or through newly defined ones. Some of these items are already under review by special	Consider a more formal IT governance structure and process that provides for business and executive level approval and support when appropriate. **Management Update:** In Progress Target Date: See items below A review of the existing structure and process has been completed. A governance matrix has been developed outlining categories of decisions, relevant IT committees and groups, and level of authority in the decision categories. The original matrix was developed and posted on the CIO website in February 2015. An updated matrix was developed in July 2015. There are several next steps to occur with regard to structure and process: ➢ Develop and implement a project approval process which includes thresholds based on impact, data, and finance. Initial scope and framework is in progress. **Target Completion Date: December 2015** ➢ Establish the following governance committees currently not in existence. o Business Systems Governance Council. Target Completion Date: **Complete** o Academic Technologies Advisory Council (title could change). **Target Completion**

Departmental Action Plan Status Form
Internal Audit of Mobile Computing Security (Issued November 2013)

campus working groups, including the Security Office, such as determining appropriate use of cloud services, appropriate use of non-UA devices and managing mobile devices. If a new more formalized IT governance structure is established, these areas will be considered accordingly.	**Date: ~~September 2015~~** MAy 2016 ○ University Executive Coordinating Group. **Complete** Complete an internal operational risk assessment for mobile computing that includes a review of policy, data storage, network security management, remote access (VPN), authentication, application management and asset management. **Management Update:** In Progress **Target Completion Date:** See items below An internal operational risk assessment for mobile computing risk will be completed. This will include a conversation with the IT Directors council, which includes IT Directors from UITS along with campus administrative and academic units. **Target Completion Date: December 2015** It is important to note that the existing security policy and guidelines includes specific references to mobile devices where appropriate. For example, the guideline for Access Control, # IS-S702, states that "All devices, including mobile devices, on which confidential university data are stored, must be kept in a physically secure location when the user or other responsible individual is not present." Additional requirements for anti-virus software, software patching, password protection, etc. are currently published on the website at security.arizona.edu. Determine the appropriate use of cloud services for storing University data. **Management Update:** Complete

	A file-sharing guide has been established outlining which sharing services can be used for each classification of data. All can be found online at http://security.arizona.edu/data-classification-and-handling-standard. Review VPN services and the type of devices permitted to access the service and if current session time-outs are appropriate. **Management Update:** In Progress **Target Completion Date:** See items below The Information Security Office has reviewed the VPN service, usage statistics, and risks. Early outcomes of this review have resulted in the following new practices: ➢ Monitoring VPN access patterns to determine illegitimate usage ➢ Requiring new accounts to have two-factor authentication enabled ➢ Beginning in May 2015 two-factor authentication was required for all VPN activity on the central VPN services. ➢ Ongoing review and adjustment to VPN services' security requirements will be an ongoing activity for the Information Security Office. ➢ A number of campus departments likely operate their own VPN or VPN-like services which were not reviewed during this process. An attempt was made to inventory such services, that effort was met with resistance and was therefore abandoned. As these services are discovered through departmental IT audits and other means the

Departmental Action Plan Status Form
Internal Audit of Mobile Computing Security (Issued November 2013)

	Information Security Office will provide guidance, as requested, for the proper operation of such services. ➢ In light of the institutional risks posed by the distributed nature of governance and decision making in areas such as network management (to include VPN services) an item has been placed on the agenda for the Executive Coordinating Committee to consider these risks and whether any changes need to be advanced institutionally. The next meeting of this group is scheduled for October 19, 2015. **Target Completion Date: October 2015** Determine the appropriate use of devices not owned by the University to conduct University business. **Management Update:** In Progress **Target Completion Date:** December 2015 This action item is still under consideration to determine an appropriate approach. This issue will be raised with the University Executive Coordinating Group. The guideline for Minimum Security for Networked Devices, #IS-S602, within the Security Policy states "These security standards apply to all *devices* connected to the *university network* used to access, store, transmit, or interface with a *university resource*." If personally owned devices are connected to the network, then policy and guidelines for access apply. Ensure that standards regarding the testing and approval of mobile apps and application development guidelines are implemented. **Management Update:** In Progress

	Target Completion Date: See items below The University has established an extensive program called Mobile Matters focused on providing guidance on the development of mobile applications. The goals of the program are to provide a place for those interested in mobile development to share ideas, find resources, and learn about best practice approaches. The program outlines rules and steps for development, resources for support, branding requirements, etc. It also outlines the steps that should be taken for development, review, and release. A campus committee, App Submission Committee, reviews all apps before release to the public. Membership includes representatives from UITS, Engineering, Tech Launch Arizona, OGC, OIA, University Relations, and Risk Management. Details about the Mobile Matters program can be found online at mobilematters.arizona.edu. The Office of the CIO, as indicated in prior audits, has considered the deployment of security vulnerability scanning tools to scan locally developed web and mobile applications. Unfortunately these efforts have not been funded and therefore developers are left to rely on the mobile application distribution channels and\or their own tools to scan their applications, if desired. In light of the institutional risks posed by the distributed nature of governance and decision making in areas such as application development and deployment (to include mobile applications) an item has been placed on the agenda for the Executive Coordinating Committee to consider these risks and whether any changes need to be advanced institutionally. The next meeting of this group is scheduled for October 19, 2015.

Departmental Action Plan Status Form
Internal Audit of Mobile Computing Security (Issued November 2013)

Target Completion Date: December 2015

Determine the requirements for managing the mobile devices as assets and ensure that configuration changes such as security updates can be managed in an automated and timely manner.

Management Update: In Progress

Target Completion Date: See items below

The existing security policy and guidelines applies to all computing assets on campus, including mobile devices. The requirements for anti-virus software, software patching, password protection, etc. are currently published on the website at security.arizona.edu. In 2014 a team of interested IT directors put a project together charged with considering the deployment of a Mobile Device Management solution to manage University owned mobile devices, and potentially personally owned devices. This team ultimately determined that the market had not matured to a point where a single solution could be deployed across multiple units, therefore units with this requirement were largely on the own.

During the August meeting of the IT Council a subgroup was formed to analyze this market again and create a proposal regarding the strengths, challenges, and risks associated with managing and supporting mobile devices. Their timeline is not yet committed, but results are expected by December 2015.

In light of the institutional risks posed by the distributed nature of governance and decision making in areas such as device management (to include mobile devices) an item has been

Departmental Action Plan Status Form
Internal Audit of Mobile Computing Security (Issued November 2013)

	placed on the agenda for the Executive Coordinating Committee to consider these risks and whether any changes need to be advanced institutionally. The next meeting of this group is scheduled for October 19, 2015. **Target Completion Date: December 2015**

The status and the description of actual corrective actions taken as described on this form are accurately reported.

Signature

9/23/15
Date

Michele Norin, CIO, 520-621-5972
Print Name, Title and Telephone Number